NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

INTELLIGENCE DISSEMINATION TO THE WARFIGHTER

by

Karin Thornton
Tim Marenic

December 2007

Thesis Advisor:	Dorothy Denning
Second Reader:	Robert O'Connell

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2007	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE Intelligence Dissemination to the Warfighter	**5. FUNDING NUMBERS**
6. AUTHOR(S) Captain Karin Thornton, USAF Captain Timothy Marenic, USAF	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

This thesis explores the intelligence cycle with emphasis on the dissemination of data from the intelligence community to forward deployed operators, also known as the warfighters. The study focuses on the bottlenecks and other flaws within the IC that may cause delays in getting intelligence reports and products in support of national security to customers around the globe. The IC has undergone several changes since the 2001 terror attacks on the United States, thanks to the 9/11 Commission and the 2004 Intelligence Reform Act. These changes have streamlined bureaucratic processes and budget allocations, but there is still a need to acquire systems and software that maximize data transfer and security. Several commercial companies have designed collaborative tools that claim to support improved data handling. Intelligence Support Server Environment (ISSE) guard is the primary tool the US Air Force employs for exchanging data between the IC and the operators. This thesis will review the advertised upgrade to ISSE along with other tools and provide an unbiased perspective on how these tools might facilitate data dissemination to the warfighters.

14. SUBJECT TERMS Intelligence dissemination, guard, cross-domain, metadata	**15. NUMBER OF PAGES** 67
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

INTELLIGENCE DISSEMINATION TO THE WARFIGHTER

Karin E. Thornton
Captain, United States Air Force
M.S., Naval Postgraduate School

Timothy Marenic
Captain, United States Air Force
M.S., Naval Postgraduate School

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
December 2007

Authors: Captain Karin Thornton
Captain Timothy Marenic

Approved by: Dorothy Denning
Thesis Advisor

Robert O’Connell
Second Reader

Gordon McCormick
Chairman, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis explores the intelligence cycle with emphasis on the dissemination of data from the intelligence community to forward deployed operators, also known as the warfighters. The study focuses on the bottlenecks and other flaws within the IC that may cause delays in getting intelligence reports and products in support of national security to customers around the globe. The IC has undergone several changes since the 2001 terror attacks on the United States, thanks to the 9/11 Commission and the 2004 Intelligence Reform Act. These changes have streamlined bureaucratic processes and budget allocations, but there is still a need to acquire systems and software that maximize data transfer and security. Several commercial companies have designed collaborative tools that claim to support improved data handling. Intelligence Support Server Environment (ISSE) guard is the primary tool the US Air Force employs for exchanging data between the IC and the operators. This thesis will review the advertised upgrade to ISSE along with other tools and provide an unbiased perspective on how these tools might facilitate data dissemination to the warfighters.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
  A. COORDINATION GAPS IN INTELLIGENCE COLLECTION AND OPERATIONAL PLANNING 1
  B. INTERAGENCY AND MULTIPLE-DOMAIN TRANSMISSION BARRIERS 3
    1. Technological Difficulties 4
    2. Associated Security Risks 8
  C. THE FOCUS AND METHODOLOGY OF THIS THESIS 9

II. FACTORS THAT SLOW INTELLIGENCE DISSEMINATION 11
  A. OVERVIEW OF INTELLIGENCE CYCLE, THE DISCIPLINES AND DISSEMINATION ISSUES 11
  B. ORGANIZATION AND REORGANIZATION OF THE INTELLIGENCE COMMUNITY 15
  C. INTELLIGENCE FAILURES 17
  D. MONEY 21

III. GUARDS AND COLLABORATIVE TECHNOLOGIES 25
  A. GUARDS 25
    1. Domain Transfers 25
    2. The Problem of Hidden Data 28
  B. COLLABORATIVE TECHNOLOGIES 29
    1. The Email Epidemic 32
    2. Wikintelligence 33
    3. Instant Messengers 37
    4. Groove 38

IV. FUTURE TECHNOLOGIES 41

V. CONCLUSION 45

LIST OF REFERENCES 49

INITIAL DISTRIBUTION LIST 53

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Intelligence Community and Their Primary Tasks...2
Figure 2. The Intelligence Cycle...........................11
Figure 3. Intelligence Discipline and Tasked OPR..........13
Figure 4. Computer Supported Cooperative Work Matrix......31

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This thesis is dedicated to intelligence professionals who have persevered through challenging times in all the corners of the globe. Combatant Commanders don't go to war without you, and even in these challenging times of budget constraints and limited resources, the community still continues to perform at an impressive level. We, as a community, will continue to perform no matter what the odds and overcome all the obstacles in our way; maintaining the most accurate and efficient intelligence community in the world.

Capt Thornton gives a hearty thank you to her son, Luke Thornton. Luke, over the past 18 months you have been patient and thoughtful. I could never have conducted all of the research and analysis without your love and cooperation. Thanks for being such a good son.

Capt Marenic would like to give special thanks to his father, George Marenic, Col. USAF (ret.). This thesis is a direct result of the ideals and values you have worked to instill in me throughout my entire life. Also, I want to give a special thanks to my wife Kelli who has encouraged me every step of the way. Lastly, thank you to my two step daughters, Caitlyn and Emily, who have taught me to never stop improving this world we live in and to always enjoy life - every moment of every day.

We both would like to thank Dr. Dorothy Denning and Dr. Bob O'Connell for allowing us to explore this topic. Without their steadfast guidance and expertise, this project would not have been possible.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. COORDINATION GAPS IN INTELLIGENCE COLLECTION AND OPERATIONAL PLANNING

Intelligence can drive national security operations, and national security operations can drive intelligence collection and reporting. The Intelligence Community (IC) and government or military operators share an interdependent partnership that is essential to United States national security. Immediately upon identification of a threat to US interest or to national security the IC is tasked to examine, analyze and further develop the knowledge base on any potential adversary. Simultaneously, the Department of Defense (DoD) delegates authority to the theater commander or the most appropriate government organization to train, organize or prepare to conduct operations against that threat as necessary.

The quality of cooperation between the IC and the operators has fluctuated since 1947, when the IC was first established. IC-Operator tension seems to rise during crises, while collaboration tends to strengthen during peacetimes. But before the external relationships can be considered, first the internal issues need to be addressed. Among the IC, there are two distinct functions. One function is collecting intelligence and the other is processing the intelligence (analyze, fuse and produce multi-source intelligence products). The major intelligence collecting and processing organizations will be discussed later. The point to make here is that there are separate organizations which collect, categorize and initially disseminate the intelligence to predetermined distribution lists for further analysis. These lists are typically established when national intelligence agencies coordinate at executive levels and commit to disseminate the preliminary intelligence to limited customers among the 16 members of the IC. (Figure 1) It is possible at this point to see the looming quandary with this process; intelligence is collected and primarily distributed to other intelligence organizations, not to the warfighters. Eventually, the intelligence is further processed and pushed to the tactical units, but there is a recognized delay.

Central Intelligence Agency	**Covert actions, global all-source collection and analysis**
National Security Agency	**Signals Intelligence, global collection and analysis of communications**
Defense Intelligence Agency	**Support to DoD and Defense Attaches**
National Geospatial-Intelligence Agency	**Prepares geospatial data, maps, charts and targeting data**
National Reconnaissance Office	**Develops and operates reconnaissance satellites**
Department of Homeland Security	**Fuses law enforcement and intelligence, counterterrorism**
Federal Bureau of Investigation	**Counterintelligence, counterterrorism**
Energy Department	**Reports on foreign nuclear weapons programs, nonproliferation**
State Department	**Analytical diplomatic reporting**
Treasury Department	**Monitors US monetary policies, terrorist financing**
Drug Enforcement Agency	**Counter-narcotics**
Air Force Intelligence	**Intelligence support to service specific missions, supplement CIA analysts on variety of technical reporting**
Army Intelligence	
Navy Intelligence	
Marine Corps Intelligence	
Coast Guard Intelligence	

Figure 1. Intelligence Community and Their Primary Tasks[1]

[1] Richard A. Best, CRS Report RL33539, *Intelligence Issues for Congress* (110th Congress), August 7, 2007.

As the IC and the tasked operators progress towards confronting the same opponent, one would think there would be an ongoing exchange of communication and coordination. Often that is not the case. Because of the latency in pushing the intelligence reports outside of the IC, operators will establish their own, seemingly more efficient intelligence resources, resulting in the IC and the operators developing independent dossiers and solutions for targets, based on their separate sources and analysis.[2] Better crosstalk and harmonization of effort is vital to synchronize the Intelligence Preparation of the Battlefield (IPB) and to maximize IC and operational efforts and assets.

B. INTERAGENCY AND MULTIPLE-DOMAIN TRANSMISSION BARRIERS

The two types of intelligence organizations were already mentioned, the collections agencies and the processing agencies. Unfortunately, within these bureaucratic organizations, there are multiple technological and security barriers that prevent the optimal exchange of data. There are even more layers of obstruction beyond the IC. Military components and paramilitary organizations require real-time intelligence but utilize various non-collaborative software and systems. In addition, customers outside of the IC have non-traditional procedures when handling and managing intelligence products, which introduces the potential for increased security risks associated with disseminating the intelligence across

[2] Tactical operators are required to complete mission reports (misreps) that are often, in turn, used by that same tactical unit to conduct Intelligence Preparation of the Battlefield (IPB). Circular reporting exacerbates the problem of tactical units disregarding national intelligence and instead using locally derived data.

multiple domains. Increased security risks cause delays in distributing sensitive data. The customer is required to verify their methods of secure data handling.

1. Technological Difficulties

Compatible technology is critical in sending customer requests for information to the collectors and disseminating intelligence to the field sites. Intelink, National Signals Database (NSD), RADIANT MERCURY and Integrated Broadcast Service (IBS) are just a few of the major systems used by the IC to transfer data. There are over 100 software programs used to disseminate intelligence between the IC and joint service customers.[3] In addition, each DoD service component maintains unique contracts and systems to communicate with interagency customers and tactical operators.

Each collection discipline was established to produce specialized intelligence products. For example, Signals Intelligence yields intercept transcripts and Imagery Intelligence generates pictures, videos and maps. These products require dedicated communication networks and bandwidth specifications which inherently limit the agencies in how they can transfer data. Once the communication lines are verified by the Defense Intelligence Agency as “secure”, the IC is held responsible to periodically validate that the dissemination is still necessary and will only transfer intelligence in accordance with national guidelines.

[3] John Pike and Steven Aftergood, “Dissemination Systems,” http://www.fas.org/irp/program/disseminate/index.html (accessed August 21, 2007).

Human error such as negligence and oversight is probably the most frustrating matter for operators. For example, the final intelligence product is available within the IC, but the warfighter down-range does not have access to it because of inadequate communication equipment, ambiguous classification guidelines or mismatched domains. Most Secret and Top Secret intelligence is freely exchanged via the Top Secret domain, the Joint Worldwide Intelligence Communications System (JWICS).[4] National intelligence organizations generally use JWICS, but tactical operators are typically limited to the Secret Internet Protocol Router (SIPRnet) domain, thus presenting a communication barrier.

It is not difficult for analysts to sanitize Top Secret reports to a Secret level, but the next step, getting the sanitized document transferred to the SIPRnet domain can be a slow, tedious process. There are two approaches to alleviate these classification roadblocks. One approach is to get the tactical users Top Secret equipment and Top Secret secure links in the field. The second approach is to streamline the process of copying the data from the Top Secret domain and placing it on the Secret domain for more effective dissemination to the tactical SIPRnet users.

There are SATCOM connections that will eventually assist tactical users in rapid mobile access to the Top Secret JWICS. Innovative tactical systems such as the SATCOM Flyaway Terminal are unfortunately still in development and are not expected to meet DoD standards for

[4] Classification levels and threats will be explained in the following section.

several years.[5] Another newly introduced device is the Remotely Operated Video Enhanced Receiver (ROVER).[6] ROVER was designed to provide streaming Top Secret full motion video to the ground troops. The MQ-1 Predator can push the real-time video via line-of-sight secure link to the ROVER which provides ground troops a video of the current battlefield as it is unfolding around them. The ROVER is not optimal in all situations, the receiving device is still over 12 lbs and the line-of-sight link limits the use in unsuitable terrain. Until the equipment is pocket size and has a more flexible data link, the ROVER will be limited to preplanned operations and reinforced combat zones.

The more effective solution is to get the data to the SIPRnet domain in a timely manner, because the greater population among tactical forces already have and routinely use SIPRnet. One method the IC uses to streamline the transmission of sanitized Top Secret data to the S domain is the Information Support Server Environment (ISSE version 3.4) guard. The ISSE system and schema will be fully explained in chapter 4, but it is useful to provide a summary of ISSE highlights.

Once data has been manually sanitized to meet SIPRnet standards, current Intelligence Directives demand that the data classification be verified before it is pushed to the

[5] L3 Communications, “Flyaway Tri-Band SATCOM Terminal,” http://www.l-3com.com/products-services/productservice.aspx?type=ps&id=214 (accessed April 10, 2007).

[6] MILTECH, “Rover Gives Joint Force New Vision,” http://www.spacewar.com/reports/ROVER_Gives_Joint_Force_New_Vision.html, December 20, 2005 (accessed August 7, 2007).

customer.[7] The automated ISSE guard scans the document and determines if it contains any Top Secret classification violations. If there are violations, the sender is notified, makes the necessary adjustments and sends it to through the ISSE guard once again. This greatly reduces the latency compared to the manual verification process used up until the late 1980s. The ISSE V3.4 is operational and has proven to be useful, but lacks an interface with e-mail and does not process all the necessary types of documents.[8]

The upgrade, designated as ISSE Star Guard, claims that it can process sanitized e-mails and several new types of documents, including RSS and XML. In addition, Star Guard has a more comprehensive procedure to verify document classification. The Star Guard has several hardware upgrades, including a faster internal processor and greater bandwidth capacity. This upgraded technology will allow the warfighter to get the intelligence faster and with less potential for classification violations. The US Air Force is currently working with the ISSE developers to determine if the upgrade will enhance intelligence dissemination.

Upgrades in technology are inevitable. Moore’s Law predicts that chip technology will continue to improve, doubling in speed every 18 months.[9] For that reason, the IC has the responsibility to evaluate these technological

[7] Director of Central Intelligence Directive 6/3, *Protecting Sensitive Compartmented Information within Information Systems*, June 5, 1999.

[8] Dolphin Technology Incorporated, ”Information Support Server Environment ISSE v3.6,” http://www.dolphtech.com/info%20sheets/ISSE3.6.pdf (accessed August 30, 2007).

[9] Gordon E. Moore, *Cramming More Components Onto Integrated Circuits,* Electronics (Volume 38, Number 8), April 19, 1965.

improvements and apply them to the intelligence cycle as necessary. Air Force Intelligence recognized the usefulness of guard technology. The ISSE guard automates the verification procedures to rapidly get sanitized data to the tactical operators on the SIPRnet, but is this the best system to use?

As chip technology improves, so must the IC continue to strive toward meeting the warfighters' demand for support in every regional conflict and provide cutting edge technological support to push transcripts, imagery, charts, audio and video intelligence products via whichever domain the customer requires. Ultimately, the point at which intelligence support ends and combat operations begin should be a seamless exchange.

2. Associated Security Risks

Security is critical when handling Top Secret, Secret and other classified data. Based on the source and sensitivity of the information, data is categorized at a specific level of classification. There are three basic levels of classification. Each level is characterized with a unique degree of damage it would cause the United States if the classified data is compromised. Confidential data would cause "damage", Secret data would cause "serious damage" and Top Secret would cause "exceptionally grave damage" to the nation if there was an unauthorized disclosure.[10] In order to handle classified data one must possess the proper security clearance, have a "need to know"

[10] Executive Order 12958, *Classified National Security Information*, March 25, 2003, Sec 1.2.

and have accounts to access the classified domains. Top Secret resides on JWICS, and both Confidential and Secret are on SIPRnet domains.

There are workarounds if the operators do not have the proper clearances. The IC, when necessary, can sanitize Top Secret data but maintain the essential elements of information and disseminate the sanitized intelligence to the customer on the SIPRnet. Generally, the data modified or removed during the sanitization process is not significant to the operator nor is it necessary to initiate a mission. It is important to note that workarounds are temporary fixes. They are used when there is time-sensitive intelligence and operations that cannot execute without it. These workarounds only emphasize that timely intelligence can make or break operations, and systems such as ISSE might facilitate better data exchange.

C. THE FOCUS AND METHODOLOGY OF THIS THESIS

This thesis addresses the problem of intelligence sharing between the IC and operators within the framework of existing intelligence directives and controls. In order to enhance the intelligence sharing, one must first identify bottlenecks and insufficiencies, some of which are exposed in this thesis. Bureaucratic factors such as the organization and reorganization of the IC will be examined. Some other factors that will be explored are the rules and processes that govern intelligence as well as the people and paradigms that degrade effective intelligence sharing.

Technological breakthroughs and upgrades have paved the way for the evolution of intelligence communication and dissemination over the last 50 years. Yet the demand to get intelligence faster, more securely, and more accurately will continue to challenge the IC. Both the current and emerging technology means of dissemination will be examined. Specifically, ISSE will be scrutinized as it is being used currently and how it may assist timely cross-domain intelligence transfer with the proposed upgrades. This thesis is not suggesting that these technological developments will solve the dissemination problems, but that they may facilitate a more timely process to transmit intelligence from the producers to the operators.

II. FACTORS THAT SLOW INTELLIGENCE DISSEMINATION

A. OVERVIEW OF INTELLIGENCE CYCLE, THE DISCIPLINES AND DISSEMINATION ISSUES

The goal for intelligence analysts is to provide accurate and timely intelligence to the warfighter.[11] The IC works within the framework of the intelligence cycle, sometimes referred to by joint military organizations as the intelligence process. After a brief summary of the intelligence cycle, the five main “Ints”, known as disciplines, will also be explained. Once these foundations for intelligence production are laid out, the challenges within the cycle as well as the bottlenecks in the dissemination process will become more evident.

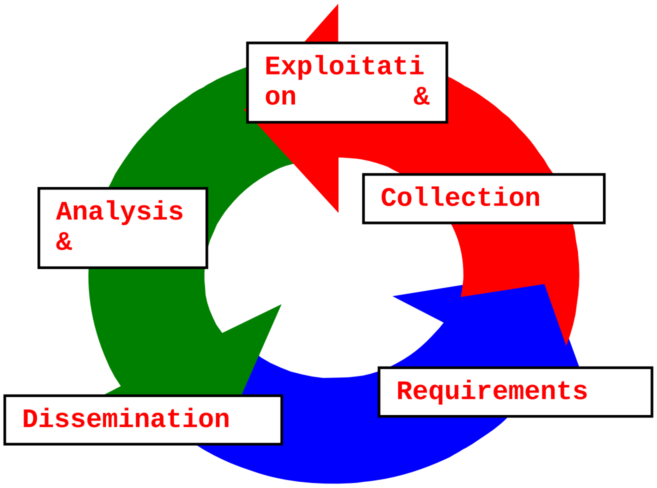


Figure 2. The Intelligence Cycle

[11] Richard A. Best, CRS Report RL33539, *Intelligence Issues for Congress* (110th Congress), August 7, 2007, 14.

According to the CIA, the five components of the intelligence cycle are: Requirements, Collection, Exploitation, Analysis and Dissemination.[12] Requirements are derived from operators needing to know more about events around the globe. For example, military or other governmental officials, more commonly known as the customer, need to know specific data that is not readily available in open sources or in accessible intelligence databases. The requirement is validated by collection managers who will determine if the desired data already exists within the IC's multiple classified databases or if the data needs to be acquired.

The validated requirement will then be married up to an "Int" or discipline and will be tasked to a specific collection platform within that discipline. Once the data is collected, an appropriate organization will then exploit and analyze the data and prepare the intelligence product for dissemination to the customer.

The 5 disciplines are: Imagery (IMINT), Signals (SIGINT), Measurement and signatures (MASINT), Human (HUMINT) and Open Source (OSINT).[13] The intelligence cycle appears to be straightforward, but of course, there's more to the process than a simple 5 spoke wheel.

The IC, in its modern iteration, has been in business for over 50 years, so why would this process be anything less than a well-oiled machine, producing and disseminating

[12] Director of Central Intelligence*, A Consumer's Guide to Intelligence* (PAS 95-00010), Washington, DC: Central Intelligence Agency, 1995, 3.

intelligence to the customer on demand? One reason is that within each discipline, there are unique procedures in prioritizing collection tasks and classifying products.

IMINT	**National Geospatial-Intelligence Agency (NGA)**
SIGINT	**National Security Agency (NSA)**
HUMINT	**Central Intelligence Agency (CIA)**
MASINT	**Defense Intelligence Agency (DIA)**
OSINT	**Foreign Broadcast Information Service (FBIS)**
	National Air and Space Intelligence Center (NASIC)

Figure 3. Intelligence Discipline and Tasked OPR[14]

In the IMINT and SIGINT disciplines, classification guidelines are clearly defined. The data is derived from sources such as reconnaissance platforms like the RC-135V/W RIVET JOINT or the U-2 Dragon Lady. There are also multiple satellites that collect both SIGINT and IMINT. The data is classified largely depending on the collection source. Generally all SIGINT and IMINT collection is initially classified as Top Secret. A program called TEAR LINES pushes the Top Secret report once it has removed sensitive elements and source data but maintained the integrity of the report, to the Secret audiences. The customer must have the approved software that supports the TEAR LINE procedures. Routine SIGINT and IMINT customers have the standard TEAR LINE programs, but when sending reports to deployed

[13] United States Intelligence Community, "Collection," http://www.intelligence.gov/2-business_cycle2.shtml(accessed September 5, 2007).

[14] OSINT is collected by several Organizations. Foreign Broadcast Foreign Broadcast Information Service and the National Air and Space Intelligence Center are not among the 16 organizations in the IC.

locations, often there are customers who are filtered out because of this software requirement.

MASINT, as a general rule, is full of technical data that cannot be sanitized. MASINT is rarely necessary in the field for tactical missions and hence does not traditionally complicate the “intelligence to the warfighter” dilemma.

HUMINT on the other hand, presents the greatest challenge. There are multiple sources, categorized by various standards, depending on which service, agency or tactical team is conducting HUMINT operations. CIA is the lead for HUMINT collection, although, specialized DoD components had a significant role in HUMINT missions in recent history. In Operation Enduring Freedom, Special Forces conducted several paramilitary operations alongside CIA operators.[15] Because of the sensitivity of these missions and the occasional covert HUMINT collection, teams handled dissemination of this data with local “need to know” classifications. Often, missions were part of special access programs and therefore the HUMINT was not forwarded to CIA main offices until operations were completed.

Since 2005, when the CIA stood up the National Clandestine Service, cooperation among the HUMINT operators has improved. The CIA Director was tasked as the National HUMINT Manager; therefore, he must coordinate not only CIA operations, but all other agencies conducting HUMINT. This additional coordination should facilitate a central repository for all HUMINT reports and provide Special Forces and other operators improved access to the data.

[15] Richard A. Best, CRS Report RL33539, *Intelligence Issues for Congress* (110th Congress), August 7, 2007, 18.

Unfortunately, some agencies use firewalls that prevent other JWICS users from exchanging data. The CIA conducts most of their business on the CIAnet, which can pull data from JWICS but blocks access from non-CIA users. Characteristically, HUMINT is stored on CIA terminals and is therefore inaccessible to standard JWICS users. Cross-domain programs such as the ISSE guard can ease the communication between the different organizations, but communications must be initiated by the more restrictive network (in this case, the CIA).

Inherently with the five disciplines, there are multiple standards of reports and processes for dissemination. Until the IC merges their networks, synchronizes software, and agrees upon a common communications system that meets the needs of all collectors and customers, there will be firewalls and incompatible security issues among the IC networks.

In addition to the network barriers between the different disciplines, there are inconsistencies within the bureaucratic processes within the IC. The 2004 Intelligence Reform reorganized the IC chain of command. The five collection disciplines and how intelligence is produced and disseminated was not affected by the reform. The next section will discuss the intelligence reform and the effects on the organization of the IC.

B. ORGANIZATION AND REORGANIZATION OF THE INTELLIGENCE COMMUNITY

Pre 9/11, the IC was organized by intelligence disciplines and further delineated by Area of Responsibility (AOR). After the devastating terrorist attacks in 2001, the

IC reorganized in accordance with the 2004 Intelligence Reform (IR).[16] The most notable difference is in the central focus on terrorism and the reorganization of assets to align trans-nationally based on the threat and not on the AOR. As noted, there are 16 members in the intelligence community. Each has specific areas of expertise and specific customers that depend on their unique capabilities and products. The National Intelligence Director (DNI) was also established to manage the national intelligence effort.

Previously, the DCI wore a dual hat as the head of the IC and Director of the CIA. There was some debate within the IC as to whether the DCI was CIA biased when producing the President's daily briefing. Now, with that function under the DNI, the CIA's input is calculated with the rest of the IC, providing a more fused product for the President.

In addition to the DNI and the 16 members of the IC, the 2004 IR established cross-border centers. These centers are created and terminated as necessary and are not limited by the regional paradigm. The National Counterterrorism Center, the Counter Proliferation Center and the National Intelligence Center are manned as necessary and tasked to track global adversaries. The missions of the Counterterrorism and Counter Proliferation Centers are self explanatory, but the National Intelligence Center's focus shifts with crises and current events in accordance with requirements of the DNI. Because these Intelligence Centers are erected by the DNI and produce and report directly on behalf of the DNI, they may be successful in avoiding the

[16] U.S. Congress, *Intelligence Reform and Terrorism Prevention Act of 2004*(108th Congress, Second Session), December 17, 2004, Sec 1011.

bureaucratic woes of the traditional intelligence organizations such as insufficient funds, scarce manning and inadequate access to all-source reporting throughout the IC.[17]

The DNI must be cautious of redundancy and wasted effort when establishing a new center based on an erupting crisis. For example, former Secretary of Defense, Donald Rumsfeld, had a knack for creating new organizations when he did not get the answers from the existing reporting cells.[18] Rumsfeld was accused of duplicating effort and tasking his "staff" to produce the same products that were assigned to the IC. The DNI centers can avoid wasteful redundancy by researching the division of labor and the IC procedures for tasking and responsibilities. Furthermore, the centers must make it a priority to interface with the IC and weigh all of the inputs from the multiple "ints" that might already be providing routine reporting on the same or parallel targets that are tasked to the temporary centers.

C. INTELLIGENCE FAILURES

How do national security critics define an intelligence failure? Is it when intelligence estimates are later reviewed and proven to be inaccurate? Is it when the military acts on current intelligence reports that detail the whereabouts of a high value target (HVT), but when an operation to kill or capture that HVT is executed, the target has moved on? Intelligence is outdated within

[17] U.S. Congress, *Intelligence Reform and Terrorism Prevention Act of 2004* (108th Congress, Second Session), December 17, 2004, Section 1014.

[18] Barton Gellman, Washington Post, *Secret Unit Expands Rumsfeld's Domain*, January 23, 2005, accessed September 12, 2007.

minutes of its collection – even with the best technology and real-time reporting, the movements and actions of people are often unpredictable. The IC monitors and reports on the here and now, but almost by definition, does not control the movements of collection targets. The concept of intelligence failure is often exacerbated by the comparison of many operational successes. Operators organize and plan missions based on the facts provided by the IC. Prompt and accurate intelligence is the backbone of every operational success. Without "good intel" these missions would not happen.[19]

Perceived intelligence failures by the customers, whether civilian or military, have harmful effects on future cooperation. When military and national security leaders receive intelligence briefings and estimates, they must understand that these briefings calculating future activities are subject to human nature and change. There is no crystal ball to ensure the 100% accuracy when predicting future events. With that said, there are analysts, sources and methods that are more accurate or more beneficial than others.

IMINT can be effective in proving numbers, assessing troop strength and providing friendly forces a dimension of the battlefield. However, IMINT does not provide adversary intentions. Conversely, SIGINT and HUMINT reports can be used to calculate and act on adversary intentions. Generally, operators would agree that HUMINT is valued over most disciplines in the Global War on Terror because of the

[19] U.S. Department of the Army, *Field Manual 100-16: Army Operational Support*, Washington, DC: Government Printing Office 1995, Section 1-1.

candid, forthright evidence gathered from one on one conversation.

Intelligence failures happen. Post 9/11 analysts reviewed transcripts and reports and found there were many indicators that could have led authorities to apprehend the 19 hijackers. Certainly, it is easier to evaluate data after the fact, when you know what you are looking for. Nevertheless, that doesn’t let the IC off the hook. Analysts are trained to notice outliers and to report on suspicious activity in order to prevent attacks, especially within the US. But there is a worse type of intelligence failure, one that is blamed on poor processes and avoidable oversight for which the IC is duly criticized. Occasionally, the IC needlessly restricts access to the operators because of ambiguous classification rules. The IC has also denied or delayed intelligence reports to operators because of technological shortcomings. In cases such as these, the intelligence failure is simply not getting the information to the customers who need it. Intelligence reports after the fact are only as valuable as news articles.

During the Vietnam War there were numerous occasions when the intelligence reports never made it to the decision makers on the ground. One example comes from the redirection of intelligence support in 1963 to big army units and conventional operations rather than continuing support to the Special Forces combating the local Viet Cong underground organizations.[20] Another example from Vietnam

[20] Andrew F. Krepinevich, jr., *The Army and Vietnam*, (The John Hopkins University Press, Baltimore and London, 1988), 230.

is the incomplete intelligence provided for the Son Tay raid. The IC provided only the details on the Son Tay compound and completely ignored any reporting on the surrounding installations. The results were dreadful. Just prior to the raid, the Viet Cong moved the POWs to a facility 400 meters south. Not a single POW was rescued because of the narrow focus and undeveloped intelligence analysis.[21] In 1960, the Bay of Pigs fiasco provides an example of CIA driven, stove-piped and biased intelligence, disseminated only to select audiences because of secrecy and politics.[22] If the IC had corroborated the findings and there had been better communication between the military and the intelligence analysts, the Bay of Pigs could have had a happier ending. These are the intelligence failures that are more detrimental to national security and degrade the reputation of the intelligence community.

The avoidable failures, such as the ones mentioned, must be addressed. Wider dissemination and timely reports to the field are objectives the IC must successfully address. There is a need for an improved dissemination system such as ISSE, which can facilitate faster and more secure transfer of data. The IC needs to reinforce to analysts that not only do they need to develop actionable intelligence reports, but it is just as essential to get the intelligence to the operators that need it. With faster and more accurate intelligence support to the customers, the

[21] William H. McRaven, *Spec Ops: Case Studies in Special Operations Warfare: Theory and Practice* (Navato, CA: Presidio Press), 1995, 287.

[22] Lucien S. Vandenbroucke*, Perilous Options: Special Operations as an Instrument of US Foreign Policy* (New York, Oxford University Press, 1993), 9-18.

interagency, inter-service trust is strengthened, which is imperative in coordinating national security operations.

D. MONEY

The Office of the DNI reviews the performance of the IC annually to ensure the members are accomplishing their assigned tasks. There are chiefly two occasions when intelligence organizations are recognized by Congress or scrutinized by the media: in times of great success or in times of dismal failure. It is logical to presume the organizations that are in the latter group have failed because of the need for manpower, resources or better equipment, but paradoxically, the organizations that often get additional funding with each annual budget proposal are the ones that have had the great successes. Among the IC it is common to see agencies competing for priority tasking because of the money pot that comes with it.

The Intelligence budget has three components. The first is the National Foreign Intelligence Program (NFIP), which primarily funds the non-DOD members of the IC. The second component is the Joint Military Intelligence Program (JMIP), which funds DoD members and some agency tasking such as the NSA, NGA and NRO in support of DoD activities. The third component, the Tactical Intelligence and Related Activities (TIARA), provides funds for tactical intelligence collection such as airborne collection platforms and deployed military collection assets.

Although the three components are already somewhat earmarked towards categorized tasking based on recurring needs, there is still room for competition when it comes to new threats, new methods and current events. When a threat emerges onto the center-stage, such as terrorism did in 2001, the members of the IC propose multiple collection and analysis plans in order to maximize the exploitation of that threat. Whatever organization receives the tasking and operates as the Office of Primary Responsibility will also get the funding to carry out the additional duties. Organizations will not only stand up the new offices needed to satisfy the added tasking, but they often use the additional funding to enhance collection analysis and reporting agency wide.

The 9/11 Commission reviewed the U.S. intelligence budget in 2004 and came up with several recommendations that they believed would empower the IC and better support the overall Global War on Terrorism.[23] Some of the suggestions are listed below:

- Establish a DNI to oversee requests and appropriations for the entire IC
- Better Congressional oversight for intelligence by establishing a committee that combines authorizing and appropriating authority
- Balance the spending among technical capabilities and human intelligence
- Prioritize National Security budget needs over individual agency specific tasking
- Reprogramming or redirecting funds after the annual budget is approved must be a joint effort between Congress and the DNI

The choke point of the IC budget is now the DNI. This appears to streamline the budget procedures compared to the

[23] Thomas J. Nicola, CRS Report RL32609, *9/11 Commission Recommendations: Intelligence Budget*, September 27, 2004.

pre-9/11 DCI process. Now, each IC entity has an equable opportunity to request annual funding. Previously, there was a perceived bias that the CIA had exclusive consideration because of the more frequent interaction of the DCI with his host organization.

How much should be spent on new and improved software, gadgets and collaborative tools? The answer is reflected in the congressionally approved annual budget. The amount is based on how well companies pitch their products to the IC. Each year various defense contractors coordinate with DoD components to develop tools and futuristic programs that can remedy shortfalls in intelligence collection, analysis, reporting and dissemination. Often, Congress and taxpayers will ask for measurable results to prove effective performance or potential for progress in exploiting and defeating threats. In 1996, the Commission on the Role and Capability of the US IC found that establishing the IC budget is not a perfect science:

> Ultimately, the Commission concluded that developing a precise criterion for measuring the right level of intelligence resources would inevitably be too simplistic and perhaps unwise. The reality, as for many functions of government, is that intelligence capabilities are determined by whatever the nation chooses to spend on them, not by some rigorous calculation which attempts to precisely balance threats against capabilities. Like the conduct of diplomacy, controlling commercial air traffic, monitoring weather, or defending our borders, there is always more that could be done. Unlike the precision that the government can attach to the cost of delivering a letter, or printing and delivering a Social Security check, there is no precise means to determine how much the nation should spend on intelligence. Just as with other

> aspects of our national security, determining the appropriate level for intelligence funding requires an assessment of various criteria such as foreign threats and the advantages a particular capability can provide against such threats. These must then be weighed against what the nation can afford, given other government spending requirements and priorities.[24]

Nevertheless, in general, the better the organization performs, the more tasking it will be assigned, which results in additional manpower and funds for that entity. That concept of performance based funding provides the foundation for the IC to continuously improve the quality and capabilities of their collection and analysis. In this competitive arena, it will be the death of an organization not to expand capabilities and refine proficiencies.

Consequently, the IC is continuously seeking to upgrade equipment and acquire commercial programs that can facilitate larger data storage, faster retrieval and transmission capability and most importantly, procure upgrades that ensure stable and secure performance. In the next two chapters several prospective systems and collaborative tools will be discussed. Does the cost of the new programs, training and maintenance support outweigh the benefits? That is what intelligence acquisition professionals must determine as they review the emerging software and quasi-autonomous systems.

[24] Commission on the Role and Capability of the US Intelligence Community, *Preparing for the 21st Century, An Appraisal of US Intelligence*, Washington D.C., US GPO, March 1, 1996.

III. GUARDS AND COLLABORATIVE TECHNOLOGIES

A. GUARDS

Today’s military demands better, faster intelligence. Millions of dollars have been spent to improve intelligence gathering devices. No longer must imagery analysts wait for photos to be developed, as high resolution, digital imagery can provide very high quality imagery. Miniaturization has also benefited the intelligence profession, as cameras and recording devices have become small enough to be carried, inconspicuously, in any situation. With the numerous advancements and technologies adopted in intelligence gathering, very little effort has been made to improve intelligence dissemination. Dissemination of intelligence requires two key components. First, the intelligence must be spread accurately and reliably to consumers in such a time that allows for action to be taken. Secondly, the sources and methods of intelligence gathering must be protected properly. Unfortunately, intelligence professionals unintentionally reveal sources of the intelligence within routine reports. Various technologies, such as guards and collaborative tools, can remedy this problem of source protection and dissemination.

1. Domain Transfers

To protect the sources and methods of intelligence gathering, information is originally classified at the level it was gathered and maintained on the proper network, typically on the Joint Worldwide Intelligence Community

System (JWICS). The main issue with machine to machine information sharing is that creating any link between different classification levels introduces the potential for unauthorized users to gain access to information that is restricted. Therefore, each classification system resides on a unique domain. The major domains used are: JWICS, Secret Internet Protocol Router Network (SIPRnet) and the Non-Classified Internet Protocol Router Network (NIPRnet).

All of the domains are physically separated from each other and only authorized users can access the appropriate domains. Previously, information was manually sanitized and downloaded onto portable media (IE floppy disk) and hand carried to a computer at the desired classification system. Obviously, this method is slow and cumbersome for today's fast paced, network centric environment. The solution to both the security and time aspect to the information sharing problem was the advent of guards.[25] A guard "acts as the information mediator between differing levels of security domains (Unclassified, Secret, Top Secret, etc). These guards continue to improve their messaging capabilities to perform functions of transliteration, sanitization, filtering, and routing based on operator needs and policy decisions".[26] One such guard that was briefly discussed in Chapter two is the Information Server Support Environment (ISSE) guard. Currently there are over 60 ISSE guard

[25] Mel Crocker, "Cross-Domain Information Sharing in a tactical Environment," Journal of Defense Software Engineering March 2007, http://www.stsc.hill.af.mil/crosstalk/2007/03/0703Crocker.html, accessed May 6, 2007. (Section on CDS)

[26] Mel Crocker, "Cross-Domain Information Sharing in a tactical Environment," Journal of Defense Software Engineering March 2007, http://www.stsc.hill.af.mil/crosstalk/2007/03/0703Crocker.html, accessed May 6, 2007. (Technology Advances, section 1)

systems in use by the DOD. Its ability to scan multiple file formats and user friendly software has made this system very valuable for the United States Air Force.[27]

An ISSE guard is a computer with two network interface cards (NIC). One NIC is plugged into the higher classification server while another is plugged into the lower classification server. The guard scans the data that travels between the two unequal domains for inappropriate information.[28]

The ISSE guard is designed to allow email transfer between the two levels of security on the domains. Once received by the guard the email is subjected to several checks to ensure no inappropriate content, including viruses, are passed between domains. If the email passes all the security checks it is then passed to the end user designated by the email. Furthermore, ISSE is able to scan files that are attached to emails in addition to the email text. This guard allows for the potential of near real-time data transfer between security levels. However, this near real-time processing requires users on both ends to be present and monitoring their user accounts. Users are subject to human obstacles, such as lunch breaks, less than 24 hour coverage or user profiles that don't allow access to specific files. These hurdles can be avoided by following

[27] Mel Crocker, "Cross-Domain Information Sharing in a tactical Environment," Journal of Defense Software Engineering March 2007, http://www.stsc.hill.af.mil/crosstalk/2007/03/0703Crocker.html, accessed May 6, 2007.

[28] Wilson Dizard and Patience Wait, "Protecting and Sharing Data: Experts Discuss Cross-Domain intelligence Swapping," GCN, April 2, 2007, http://www.gcn.com/print/26_07/43404-1.html (accessed May 6, 2007.

standard procedures of monitoring communications and maintaining standard computer profiles and configurations.

2. The Problem of Hidden Data

The most dangerous issue that exists with guard technology is eliminating hidden data. Spreadsheets and word processors, in order to retain a high level of user-friendliness, handle several complex background processes that create hidden data, unbeknownst to the creator. Hidden data, which includes metadata, must be removed prior to dissemination because it can, with the skills of computer savvy analyst, be uncovered by users not cleared for such data.

Metadata is prevalent when there are multiple authors of a document. When an analyst modifies a source document and saves the changes, metadata remains in the file. The standard procedure is to create a new document and only copy what is appropriate for the intended distribution list. Most guards only scan the surface text of these documents and therefore such hidden data is still able to pass boundaries.[29] One solution to minimize the hidden data risk is to program the guard to reject any document that is capable of containing retrievable metadata. This limitation might impede some intelligence exchange, but it would also standardize document types and formats, establishing a more efficient transfer process.

Purifile is a dissemination tool that alleviates the problem of transferring unseen data. Purifile was

[29] Ronald Hackett, “Hidden Data: You May Be Sharing More than You Think,” August 21, 2006, http://federaltimes.com/index.php?S=2044545 (accessed May 3, 2007).

specifically designed to identify and remove hidden data from Microsoft products.[30] Purifile was recently named a 2007 "Category Breaker", in addition to receiving other awards, by Network World for its ability to not only detect hidden data, but also to discover embedded MS Office files, executables and macros.[31] Using Purifile would allow the IC to be more inclusive in document transfer and have less document type restrictions when disseminating intelligence reports that are filtered through a guard.

Even though some issues exist within guards, such as classified email exchange delays due to human error or gaps in shift work, or potential disclosure of hidden data or metadata, standard operating procedures among the IC can drastically limit the seriousness of the flaws in the guard systems. Therefore, guards, such as ISSE, continue to be a solid choice. Guards are arguably the fastest way of disseminating vital information across domains. However, getting intelligence onto the correct domain only solves half of the dissemination problem. Once the information is downgraded, intelligence professionals still need to be able to quickly disseminate data to a wide number of operators.

B. COLLABORATIVE TECHNOLOGIES

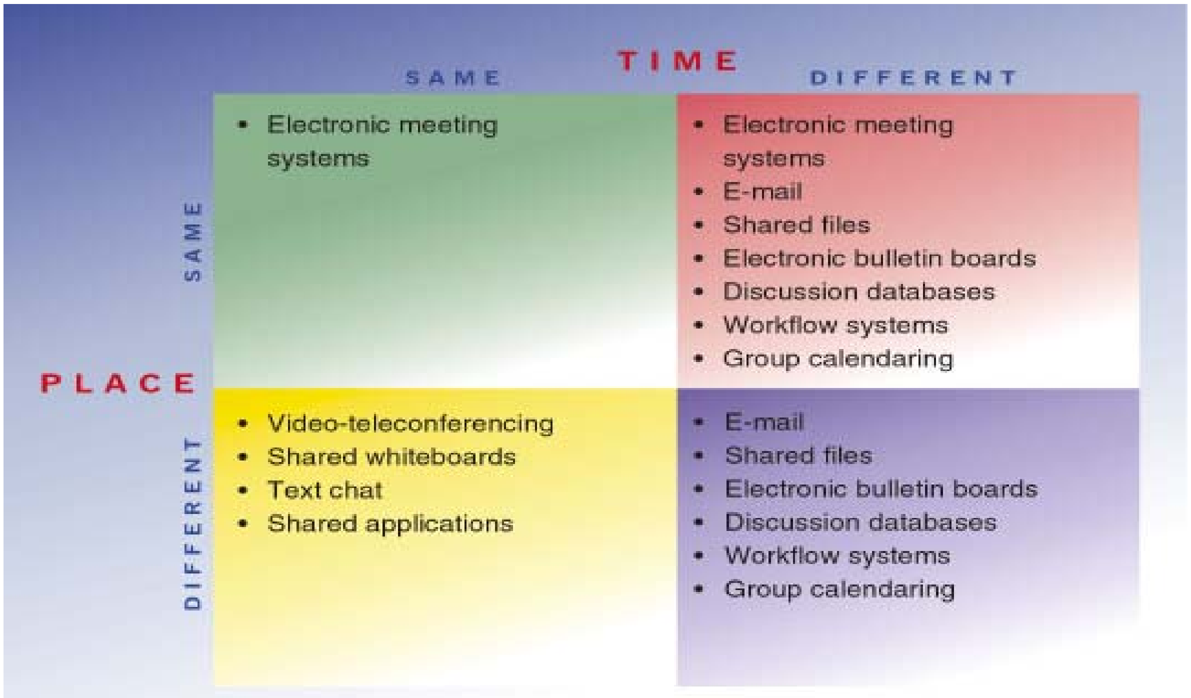
Collaboration is defined as "a process characterized by the recursive interaction of knowledge and mutual learning between two or more people who are working together, in an

[30] Winn Schwartau, "07 Category Breaker Award," http://www.networkworld.com/bestproducts/2007/022607-best-products-07.html (accessed November 10, 2007).

[31] Peter Stevenson, Dolphin Technology Purifile V3.1.3, November 1, 2007, http://www.scmagazineus.com/Dolphin-Technology-PuriFile-v313/Review/1134/ (accessed November 13, 2007).

intellectual endeavor, toward a common goal which is typically creative in nature.”[32] With respect to information technology, Computer Supported Cooperative Work (CSCW) leverages technology to facilitate collaboration. Email, wikis, instant messengers and blogs are all examples of collaborative software. CSCW tools fall into one of four categories; those that allow same time/same place collaboration, those that allow same time/different place collaboration, those that allow different time/same place collaboration, and those that allow different time/different place collaboration as seen in the following figure.

[32] Wikipedia, “Collaboration,” http://en.wikipedia.org/wiki/Collaborative (accessed November 13, 2007).



TIME

PLACE

	SAME	DIFFERENT
SAME	• Electronic meeting systems	• Electronic meeting systems • E-mail • Shared files • Electronic bulletin boards • Discussion databases • Workflow systems • Group calendaring
DIFFERENT	• Video-teleconferencing • Shared whiteboards • Text chat • Shared applications	• E-mail • Shared files • Electronic bulletin boards • Discussion databases • Workflow systems • Group calendaring

Figure 4. Computer Supported Cooperative Work Matrix[33]

With the exception of email, collaborative tools are largely shunned by the intelligence community. With the lack of collaboration, the result is typically analysis accomplished in a vacuum and the product occasionally being distributed to a limited audience. This narrow source process is time consuming, incomplete and wasteful. Uncorroborated intelligence is often regarded as having little usable data and without the use of fused reports, is typically outdated by the time it reaches the operator.

[33] R.M. Baecker and Buxton Grudin and S. Greenberg, "Readings in Human-Computer Interaction: Towards the Year 2000", 1995, (Second Edition), http://www.it.bton.ac.uk/staff/rng/teaching/notes/CSCWgroupware.html, (accessed November 13, 2007).

intellectual endeavor, toward a common goal which is typically creative in nature."[32] With respect to information technology, Computer Supported Cooperative Work (CSCW) leverages technology to facilitate collaboration. Email, wikis, instant messengers and blogs are all examples of collaborative software. CSCW tools fall into one of four categories; those that allow same time/same place collaboration, those that allow same time/different place collaboration, those that allow different time/same place collaboration, and those that allow different time/different place collaboration as seen in the following figure.

[32] Wikipedia, "Collaboration," http://en.wikipedia.org/wiki/Collaborative (accessed November 13, 2007).

from useful communications and filter out these unwanted or unnecessary emails in order to maintain effective communications. Classified domains are not subject to the same spam problem, but with auto distribution lists, email can amass quickly. Operators may receive several products from multiple agencies and because of the information overload, fail to see the few reports that had time-sensitive intelligence. Finally, email is a different time/different place collaborative tool; therefore, intelligence exchange may have to wait until both the sender and the receiver are available.

2. Wikintelligence

A wiki is another type of different time/different place collaborative tool. As defined by Wikipedia, a wiki is a “collaborative website which can be directly edited by anyone with access to it, and provides an easy method for linking from one page to another.”[37] This online, collaborative, continuously updated, encyclopedia has had exponential growth since it’s inception in 1994.[38] While the idea of granting anyone with computer access the ability to edit “at will” is precarious, the results have been phenomenal.

In 2005, a wiki was established on the JWICS domain, called Intellipedia. The idea was innovative, but the results have been disappointing. Unfortunately, Intellipedia is basically still a shell with only minimal

[37] Wikipedia, “Wiki,” http://en.wikipedia.org/wiki/Wikis (accessed November 10, 2007).

[38] Wikipedia, “What is Wiki,” Wiki.org, http://www.wiki.org/wiki.cgi?WhatIsWiki (accessed November 2007).

input. Intellipedia is not supported or encouraged by a parent organization in the IC, therefore, is not getting any substantial contribution.

A robust intelligence wiki could provide an online repository that facilitates quick edits and updates that are viewed in near real-time for local and deployed customers.[39] Instead of relying on daily briefs or scheduled updates from the IC, operators could access the wiki whenever necessary and get the information needed for current operations. "Dissemination" of actionable intelligence would be near instantaneous.

Wikis also provide a unique cooperation between analysts from various intelligence organizations. The unrestricted nature of wikis circumvents the bureaucratic layers that often prevent interagency collaboration.[40] Wikis, along with blogs, instant messaging, email and many other tools are adaptive and flexible. Input ebbs and flows with the environment, priorities and current events. According to D. Calvin Adrus, a wiki should be considered only part of the "complex adaptive systems", where the onus is placed equally on the analyst and on the tools to be receptive and adaptable. It is the responsibility of the analyst to combine these interdependent collaborative tools in order to provide multi-source, real-time, intelligence to the warfighter.[41]

[39] Edits must be provided by credible sources. Once a source is verified, unrestricted edits are permitted.

[40] D. Calvin Adrus, "The Wiki and the Blog: Toward a Complex Adaptive Intelligence Community," http://papers.ssrn.com/sol3/papers.cfm?abstract_id=755904, abstract (accessed November 12, 2007).

[41] Andrus, "The Wiki and the Blog," 24.

The IC has struggled with providing timely and accurate cultural intelligence for conflicts around the globe. With the cooperation of academia and corporate allies, the IC could establish a wiki designed to provide aspects of culture, politics and anthropologic data. Analysis of societal and economic data is often left out of the target dossier. Wikis could be the missing link for the cultural intelligence that is lacking in today's war.[42]

It would be optimal to give certain academia and corporate facilitators access to the classified wikis, but unfortunately the process of granting security clearances to such a large audience of non intelligence professionals would be complicated and costly.

Critics of the Intelligence wiki raise some valid points in using wikis as a "one stop shop". One criticism stems from clearance levels and cross domain exchanges for each topic. Most intelligence collection and analysis is done at the Top Secret level but the operators that need the data are generally only cleared to Secret. Also, wikis must be established and routinely updated at each classification level in order to maximize the exploitation of specific topics and to get the data to the warfighter in a timely manner. In 2005, the DNI was tasked with improving open source access to the IC.[43] The Open Source Center was created to merge multiple unclassified news centers and make the data available in wiki format. Most intelligence

[42] Matt Zahn and Wayne Lasey, "Building a Virtual Cultural Intelligence Community," Naval Postgraduate School thesis, June 2007, 25.

[43] The 9/11 Commission also noted that the IC was "severely deficient" at gathering open source intelligence.

analysts are familiar with reports from the Foreign Broadcast Information Center (FBIS); the Open Source Center absorbed FBIS tasking and expanded the collection of such unclassified information within the wiki.[44] Operators will agree that a "one stop shop" for open source data will improve situational awareness, but the IC must not forget that an open source wiki is not a replacement for thorough research. Furthermore, open source must be combined with multiple sources and "ints" to determine the validity of the reports.

The Open Source Center restricts access to government related personnel and attempts to validate users as U.S. citizens or government employees. A logon and password is required, but despite the security measures applied to the unclassified website, the risk of disclosure and hacking is not only possible, but probable. Therefore, inputs on the open source wiki will be, according to Executive Order 12958, restricted to information that does not pose any risk to national security, if compromised.

Even though the IC is skeptical of a merged, multi-source data repository, wikis have the potential to be a valuable resource for intelligence professionals and deployed operators. The Open Source Center's wiki will certainly aid in data dissemination on the NIPRnet. If Intellipedias on SIPRnet and JWICS become as populated and comprehensive as Wikipedia the IC might finally bridge the gap between intelligence producers and intelligence customers.

[44] Open Source Center, wiki, https://www.opensource.gov (accessed November 18, 2007).

3. Instant Messengers

Instant messengers are same time/different place collaborative tools rising in popularity. Instant messaging programs are almost as common as email for electronic communication.[45] With the continuous upgrades in instant messaging capabilities as well as the wide range of compatibility among operating systems it is no surprise that this real-time chat tool is only second to email when comparing quantities of electronic communications. Cellular phone companies are catching on to the phenomenon. Most cell phone plans now come with standard text and instant messaging services. This real time tool offers several advantages to the intelligence community.

The primary advantage provided by instant messengers is the speed of information sharing. During an instant messaging or chat session all users are online, or actively monitoring the session in one virtual space. This allows for the data to be transferred and read instantly, as opposed to email where, unless the exchange is prearranged for a set time, it is not guaranteed that the intended receiver will be present. Furthermore, messaging chat sessions are a valuable tool to actively exchange real time information and provide in depth analysis simultaneously as situations unfold. In addition to text, instant messaging programs are incorporating video and voice to their programs which will greatly enhance collaboration among users.

[45] DM Review Editorial Staff, “Email Study Reveals Trend in Usage,” http://www.dmreview.com/article_sub.cfm?articleId=1044771 December 1, 2005 (accessed November 13, 2007).

The speed of instant messengers is also one of its greatest disadvantages. With email communication a user has time to read and absorb any information or intelligence request submitted. With instant messengers, however, users are communicating in real time with the expectation to deliver the information now, as opposed to taking the time to research and possibly providing a more comprehensive analysis. Also, email has a greater capacity to send attachments such as word documents, power point presentations and imagery that the end user can peruse at their leisure. While some updated messenger services provide an ability to attach small files most are limited to simple, either text or voice based, real time communications. Despite these limitations, instant messengers remain a viable collaborative means that can be utilized by intelligence professionals. The speed of information delivery and concurrent amplification is essential to tactical decision makers, where timely answers are vital. When rapid delivery is not as crucial, collaborative tools such as email might be more effective for both operators and intelligence professionals.

4. Groove

Unlike the aforementioned collaborative tools, Microsoft Office Groove, simply referred to as Groove, resides in two areas of the collaborative tools matrix. Unique features, such as application sharing and open access workspace enable different time/different place collaboration. In addition, Groove offers a chat feature that can enable same time/different place collaboration. Groove is a peer to peer collaborative tool that enables users to create a shared workspace for multiple user collaboration. This workspace is a repository where users can place all relevant information for an ongoing project.[46] The actual data is stored on each member's personal computer which facilitates fast document retrieval. Users can also update and add to the project and post the new information to the workspace individually.

Groove presents many practical features that are not offered in traditional email or instant messengers. First, the peer to peer nature of Groove eliminates the possibility of a single point of failure for data loss. Instead, data is kept on the machines of individual users automatically, as opposed to the manual method or server storage employed by most email tools. Next, Groove allows users to efficiently change a stored document; the changes are immediately posted to the workspace and all of the users are notified that there is an updated version of the document available. Both of these features ensure the latest analysis is available to multiple operators in multiple locations around the globe. Finally, the built-in chat mode, like the instant messenger, allows for real-time coordination and clarification of intelligence reports.

There is one major disadvantage with implementing Groove. The program's size and bandwidth are more demanding than most applications. Computer networks among the IC will have no problem using the application, but deployed operators using field laptops might not have the memory or

[46] Stephen Burdian and Jadon Klopson, "Collaborative Applications used in a Wireless Environment at Sea for use in Coast Guard Law Enforcement and Homeland Security Missions," Master's Thesis, Naval Postgraduate School, 17.

connection speed required. The minimum requirements for Groove are 52 kilobit per second modem, 256 megabits of RAM, and a 400 megahertz processor, however, a high-speed connection, such as a cable modem, and 512 megabits of RAM are needed for full optimization. Groove has incorporated several features to optimize bandwidth, but this area still has room for improvement.[47]

Overall, Groove’s collaboration features, along with the common applications such as calendar and project manager, make it a very powerful intelligence analysis and dissemination tool. In fact, Groove is currently being used in such a manner by the Department of Homeland Security, in support of high profile events, such as the Republican and Democratic National Conventions.[48]

[47] Stephen Burdian and Jadon Klopson, “Collaborative Applications used in a Wireless Environment at Sea for use in Coast Guard Law Enforcement and Homeland Security Missions,” Master’s Thesis, Naval Postgraduate School, 21-24.

[48] Stephen Burdian and Jadon Klopson, 28.

IV. FUTURE TECHNOLOGIES

There are several emerging collaborative tools that might facilitate analysis and dissemination for Intelligence Community. One such tool is the Small Unit Situational Awareness tool (SUSA). The SUSA system is a stand alone operating system and does not have long term storage or fusion functions that integrate with other systems such as Groove. The SUSA does, however, provide the ability to process, analyze and exchange situational awareness information within a small tactical team. The SUSA system shares real-time situational and geographical data between the SUSA team leader, the SUSA team members and a Tactical Operations Center. The SUSA system provides each member of the tactical team with the following capabilities:

- Provides teams with real-time individual tracking.
- Allows users to mark pinpoint locations on a map using a system stylus.
- Promotes the use of multiple situational and graphical databases that can be shared across the network.
- Enhances battlefield management through extensive mapping utilities.
- Extends the communication network through the use of handheld sized data radios or WI-FI capability. The messaging utility provides an additional means of sending and receiving tactical orders, reports and information while in the field.
- Enables teams to view and share data regarding the hostile situation.

When used in a networked command center environment, the SUSA application provides each member of the tactical team with a Common Relevant Operational Picture (CROP).

Each user on the tactical network can then customize the CROP for his particular role by using a variety of re-configurable toolbars. Distributed planning is accomplished via creating a file, sharing it with the other players on the network, and then allowing the other players to "mark up" the shared plan. This sharing is a real-time interactive planning capability which allows multiple role players to simultaneously build and alter a tactical plan utilizing white board technology.[49]

The SUSA system allows operators to communicate in a free-form instant message manner, to submit/receive standard reports and message traffic and to generate and share operational graphics. Although the current SUSA system does not allow for audio/video communications between the SUSA team members, future systems are in the works that would incorporate voice and full motion video.

One final tool worth discussing is the Collaboration Gateway (CG). CG is a tool that allows for multilevel, cross-domain collaboration[50]. CG is the final piece of the puzzle that connects both guard and collaborative technologies for rapid intelligence dissemination across security levels. Instead of actively screening for unauthorized data as the ISSE does, the CG instead monitors, sorts and temporarily stores data as it flows between domains.

[49] CHI Systems Incorporated, *User Manual for GPS-Denied Navigation & Mapping System (SOF Tracker)*, July 15, 2007.

[50] John Teresko, “Technologies Of The Year, Proficiency Inc.'s Collaboration Gateway,” December 1, 2004, http://www.industryweek.com/CurrentArticles/asp/articles.asp?ArticleId=1708 (accessed November 13, 2007).

Not only does it claim to rapidly push data between domains, it can also serve as a temporary back-up for data retrieval.

Technology has provided a number of tools beneficial to the IC. Cross-domain guards, like ISSE and STAR, ensure that vital information is protected while allowing a means to transfer useful intelligence to operators on lower classification systems. Also, various collaborative technologies can aide intelligence professionals in quickly disseminating actionable intelligence. While flaws do exist in current guard and collaborative technologies, none are so serious that they cannot be overcome with proper practices. If the intelligence community, however, is unwilling to embrace current and future technologies, such as the Collaboration Gateway, intelligence failures will become more frequent while operational successes will dwindle.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

Since 2001, the Intelligence Community has been scrutinized by Congress, by government decision makers and by general pubic. Several changes were made over the last six years based on the 2004 Intelligence Reform Act and other legislation enacted post 9/11. The common notion in analyzing how the IC conducts business is the concept that the Intelligence Community should always seek to provide the most accurate and actionable intelligence to the operational customers, especially to the customers forward deployed, also known as the warfighters. Furthermore, the intelligence professionals must ensure that the data transfers to each and every customer are secure, but not at the expense of delaying the process.

The IC was reorganized in 2004 and has a modified chain of command. The DNI position was designed to remedy and streamline authorities and procedures. With a more efficient hierarchy, the DNI theoretically will have a better perspective on which organizations are performing well, and which are more suited to take on new tasking. The competition among the IC, as pointed out in chapter two, will force organizations to continuously progress.

Amid the 16 organizations of the IC, there are numerous systems and domains that each organization primarily uses. Unless the IC is mandated to merge domains, there must be workarounds and multiple methods to exchange data within and beyond the IC. There needs to be effective and systematic practices to send data from the Top Secret realm down to the users on the SIPRnet and NIPRnet domains and vice versa.

The difficulty in cross-domain exchange is at the pinnacle of bottleneck delays when it comes to getting the right intelligence to the right customer in order to exploit and affect adversaries in today's global war on terrorism. Therefore it is critical to the DoD and the Intelligence Community to seek out the best solutions to advance data transfer and data security.

In search of the best programs and equipment to support the warfighter, several commercial companies have designed products that facilitate data transfer and automated data analysis. Chapters three and four discuss the potential tools that the military and the Intelligence Community can procure. Email and instant messaging were the first of many tools to ease communication between operators down-range and the IC, facilitating a quick link for the initial flow of information. Wikis in the classified arena have potential, but must be supported, populated and maintained before they can be fully appreciated by analysts and operators. Groove and SUSA offer features that can generate more integrated, in-depth exploitation as well as provide near real-time communication. The few ISSE guard systems that are being used across the IC have proven to ease the bottleneck in data transfer to the warfighter since its inception in 1998. The new and improved ISSE guard looks promising, but will have to compete with the other data guard candidates and collaborative tools on the market. It is paramount that the leadership of the IC ensures that analysts have multiple collaborative tools available, and the analysts must be proactive in maximizing these tools to exploit the adversaries. In WWII the Germans were the first to use radar and advanced navigation tools.[51] The British first employed collection and decryption systems at Bletchley Park.[52] The US was the first to develop the atom bomb.[53] As history demonstrates, the implications of cutting edge technology may not have won wars, but did impact strategies and benefited the users by staying one step ahead of the enemy. Accordingly, today's Intelligence Community must seek out cutting edge tools in order to stay one step ahead of the enemy.

[51] Robert O'Connell, *Soul of the Sword* (Free Press, August 27, 2002), 286-292.

[52] F.H. Hinsley and Alan Strip, *Codebreakers: The Inside Story of Bletchley Park* (Oxford University Press, USA, June 21, 2001), 312-320.

[53] Robert O'Connell, *Soul of the Sword* (Free Press, August 27, 2002), 320-322.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Andrus, Calvin. (2004).“The Wiki and the Blog:Toward a Complex Adaptive Intelligence Community.” Retrieved on November 12, 2007 from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=755904.

Baecker, R.M. and Grudin, Buxton and Greenburg. (1995). “Readings in Human-Computer Interaction:Towards the Year 2000.” Second Edition. Retrieved on November 13,2007 from http://www.it.bton.ac.uk/staff/rng/teaching/notes/CSCWgroupware.html.

Best, Richard. (2007).CRS Report RL33539. *Intelligence Issues for Congress*,110th Congress.

Burdian, Stephen and Klopson, Jadon. (2007). “Collaborative Applications used in a Wireless Environment at Sea for use in Coast Guard Law Enforcement and Homeland Security Missions.” Master’s Thesis, Naval Postgraduate School.

CHI Systems Incorporated. (2007). *User Manual for GPS-Denied Navigation & Mapping System:SOF Tracker.*

Commission on the Role and Capability of the US Intelligence Community. (1996). *Preparing for the 21st Century, An Appraisal of US Intelligence*, Washington D.C., US GPO.

Crocker, Mel. (2007). “Cross-Domain Information Sharing in a tactical Environment.” Journal of Defense Software Engineering March 20076,2007 from http://www.stsc.hill.af.mil/crosstalk/2007/03/0703Crocker.html.

Director of Central Intelligence. (1995). *A Consumer’s Guide to Intelligence*. PAS 95-00010. Washington, DC: Central Intelligence Agency.

Director of Central Intelligence Directive 6/3. (1999). *Protecting Sensitive Compartmented Information within Information Systems*. Washington, DC: Central Intelligence Agency.

Dizard, Wilson and Wait, Patience. (2007). “Protecting and Sharing Data: Experts Discuss Cross-Domain intelligence Swapping.” GCN. Retrieved on May 6, 2007 from http://www.gcn.com/print/26_07/43404-1.html.

DM Review Editorial Staff. (2005). “Email Study Reveals Trend in Usage.” Retrieved on November 13, 2007 from http://www.dmreview.com/article_sub.cfm?articleId=1044771.

Dolphin Technology Incorporated. (2006). ”Information Support Server Environment ISSE v3.6.” Retrieved on August 30, 2007 from http://www.dolphtech.com/info%20sheets/ISSE3.6.pdf.

Executive Order 12958. (2003). *Classified National Security Information*.

Gellman, Barton. (2005). Washington Post. *Secret Unit Expands Rumsfeld’s Domain.*

Hackett, Ronald. (2006). “Hidden Data: You May Be Sharing More than You Think.” Retrieved on May 3, 2007, from http://federaltimes.com/index.php?S=2044545.

Hinsley, F.H. and Strip, Alan. (2001). *Codebreakers:The Inside Story of Bletchley Park*. Oxford University Press, USA.

Krepinevich, Andrew F., jr. (1988). *The Army and Vietnam*. John Hopkins University Press. Baltimore and London.

L3 Communications. (2007). “Flyaway Tri-Band SATCOM Terminal.” Retrieved on April 10, 2007, from http://www.l-3com.com/products-services/productservice.aspx?type=ps&id=214.

McRaven, William. (1995). *Spec Ops: Case Studies in Special Operations Warfare:Theory and Practice.* Navato, CA: Presidio Press.

MILTECH. (2005). “Rover Gives Joint Force New Vision.” Retrieved on August 7, 2007, from http://www.spacewar.com/reports/ROVER_Gives_Joint_Force_New_Vision.html.

Moore, Gordon. (1965). *Cramming More Components Onto Integrated Circuits,* Electronics. Volume 38, Number 8.

Nicola, Thomas. (2004). CRS Report RL32609, *9/11 Commission Recommendations: Intelligence Budget.*

O’Connell, Robert. (2002). *Soul of the Sword*. Free Press.

Open Source Center. (2007). Wiki. Retrieved on November 18, 2007, from https://www.opensource.gov.

Pike, John and Aftergood, Steven. (2007). “Dissemination Systems.” Retrieved on August 21, 2007, from http://www.fas.org/irp/program/disseminate/index.html.

Schwartau, Winn. (2007). “07 Category Breaker Award.” Retrieved on November 10, 2007, from http://www.networkworld.com/bestproducts/2007/022607-best-products-07.html.

Stevenson, Peter. (2007). “Dolphin Technology Purifile V3.1.3.” Retrieved on November 13, 2007, from http://www.scmagazineus.com/Dolphin-Technology-PuriFile-v313/Review/1134.

Teresko, John. (2004). “Technologies Of The Year, Proficiency Inc.'s Collaboration Gateway.” Retrieved on November 13, 2007, from http://www.industryweek.com/CurrentArticles/asp/articles.asp?ArticleId=1708.

United States Congress. (2004). *Intelligence Reform and Terrorism Prevention Act of 2004.* 108th Congress, Second Session.

United States Department of the Army. (1995). *Field Manual 100-16: Army Operational Support*, Washington, DC: Government Printing Office.

United States Intelligence Community. (2007). “Collection.” Retrieved on September 5, 2007, from http://www.intelligence.gov/2-business_cycle2.shtml.

Vandenbroucke, Lucien. (1993). *Perilous Options: Special Operations as an Instrument of US Foreign Policy*. New York, Oxford University Press.

Whittaker, Bellotti and Moody, P. (2007). “Revisiting and Reinventing email, Human Computer Interaction 20." Retrieved on November 13, 2007, from http://hci-journal.com/editorial/si-email-intro.pdf.

Wikipedia. (2007).“Collaboration.” Retrieved on November 13, 2007, from http://en.wikipedia.org/wiki/Collaborative.

Wikipedia. (2007). “What is Wiki,” Wiki.org. Retrieved on November 13, 2007, from http://www.wiki.org/wiki.cgi?WhatIsWiki.

Wikipedia. (2007). “Wiki.” Retrieved on November 10, 2007, from http://en.wikipedia.org/wiki/Wikis.

Zahn, Matt and Lasey, Wayne. (2007). “Building a Virtual Cultural Intelligence Community.” Naval Postgraduate School.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. JSOU
   James.D.Anderson@hurlburt.af.mil
   Hurlburt Field, Florida

4. ASD/SOLIC
   Garry.reid@osd.mil
   Washington D.C.

5. SOCOM J-7
   ballarbl@socom.mil
   Tampa, Florida

6. HQ USSOCOM Library
   taitt@socom.mil
   Tampa, Florida